Remarks

Applicants respectfully request reconsideration of the present U.S. Patent application as amended herein. Claims 28 and 39 have been amended. No claims have been added or canceled. Thus, claims 28-47 are pending.

CLAIM REJECTIONS – 35 U.S.C. § 112, SECOND PARAGRAPH

Claims 28 and 39 were rejected as being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. Claims 28 and 39 have been amended as suggested in the Office Action. Accordingly, Applicants request that the rejection of claims 28 and 39 as being indefinite be withdrawn.

CLAIM REJECTIONS – 35 U.S.C. § 103(A) – CLAIMS 28, 32 AND 33

Claims 28, 32 and 33 were rejected as being unpatentable over U.S. Patent No. 4,316,055 issued to Feistel (*Feistel '055*) in view of Schneier, "Applied Cryptography," 2nd Edition (*Applied Crypto*). For at least the reasons set forth below, Applicants submit that claims 28, 32 and 33 are not rendered obvious by *Feistel '055* and *Applied Crypto*.

Applicants agree with the Office Action that *Feistel '055* does not teach the stream cipher key section modifying the block cipher key. However, the characterization of *Feistel '055* in the Office Action is incorrect in at least one key aspect. Therefore, even if, for the sake of argument, the combination is proper and the remaining characterization of *Feistel '055* and the characterization of *Applied Crypto* is accurate, the combination cannot result in the claimed invention. Specifically, the Office Action states:

> Moreover, since ***the stream cipher key and the block cipher key are one and the same*** in Feistel (see Feistel, Figure 2a, Reference 3), and the values of the shift register in Schneier come from the modified key value derived form the block cipher key, the invention of Feistel modified by Schneier covers a stream cipher key section modifying the block cipher key according to a stream cipher key.

See page 5 (emphasis added).

However, the stream cipher key and the block cipher key of *Feistel '055* are ***not*** the same. A key value labeled "key-2" is loaded into the Main Shift Register (MSR) for use in ***stream*** encipherment. See col. 10, lines 43-49 (emphasis added). In contrast, for ***block*** encipherment, the MSR is loaded with key-2 modulo-2. See col. 12, lines 57-62. Therefore, the characterization of the cipher keys of *Feistel '055* are incorrect and the resulting combination cannot result in the invention as claimed in claim 28.

Claims 32 and 33 depend from claim 28. Because dependent claims include the limitations of the claims from which they depend, Applicants submit that claims 32 and 33 are not rendered obvious by *Feistel '055* and *Applied Crypto* for at least the reasons set forth above.

CLAIM REJECTIONS – 35 U.S.C. § 103(A) – CLAIMS 29-31, 34-37, 39 AND 41-47

Claims 29-31, 34-37, 39 and 41-47 were rejected as being unpatentable over *Feistel '055* in view of U.S. Patent No. 3,798,360 issued to Feistel (*Feistel '360*). For at least the reasons set forth below, Applicants submit that claims 29-31, 34-37, 39 and 41-47 are not rendered obvious by *Feistel '055* and *Feistel '360.*

Claims 29-31 and 34-37 depend from claim 28 discussed above. As discussed above, *Feistel '055* does not teach or suggest the stream cipher key section modifying the block cipher key. *Feistel '360* is not cited to teach, nor does it teach, this limitation.

Accordingly, no combination of *Feistel '055* and *Feistel '360* can teach or suggest the invention as claimed in claims 29-31 and 34-37.

Claim 39 recites:

> a first key section to be enabled in a stream cipher mode and disabled in a block cipher mode, and to selectively modify a cipher key into a selectively modified cipher key;
>
> a second key section to be coupled with the first key section in the stream cipher mode, and having a first, second, and third registers to be collectively initialized with the cipher key, and transformation units coupled with the first, second, and third registers to recursively transform the selectively modified cipher key into a transformed selectively modified cipher key;
>
> a data section coupled with the second key section, having a fourth, fifth, and sixth registers to be collectively initialized with a data bit sequence, and transformation units coupled with the fourth, fifth, and sixth registers to transform the data bit sequence into a transformed data bit sequence according to the transformed selectively modified cipher key; and
>
> a mapping section coupled with the second key section and the data section to generate a pseudo random bit sequence with the transformed data bit sequence.

Feistel '360 discloses a group of registers. However, the use of the registers is different in *Feistel '360* than the invention as claimed in claim 39. Because *Feistel '055* does not disclose a group of registers in this manner or even a use for such registers and *Feistel '360* proposes a different use for the registers, no combination of *Feistel '055* and *Feistel '360* can teach or suggest the invention as claimed in claim 39.

Claims 41-47 depend from claim 39. Because dependent claims include the limitations of the claims from which they depend, Applicants submit that claims 41-47 are not rendered obvious by *Feistel '055* and *Feistel '360* for at least the reasons set forth above.

CLAIM REJECTIONS – 35 U.S.C. § 103(A) – CLAIMS 38 AND 40

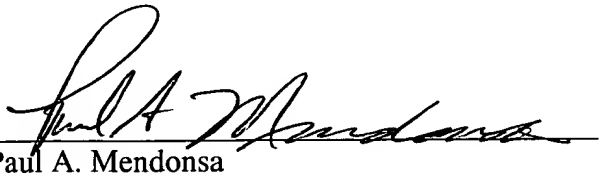
Claims 38 and 40 were rejected as being unpatentable over *Feistel '055* in view of U.S. Patent No. 4,641,102 issued to Coulthart (*Coulthart*). Claims 38 and 40 depend from claims 28 and 39, respectively, which have been discussed above. *Coulthart* is cited to teach an unbiased random number generator. However, *Coulthart* does not cure the deficiencies of *Feistel '055* set forth above. Therefore, no combination of *Feistel '055* and *Coulthart* can teach or suggest the invention as claimed in claims 38 and 40.

CONCLUSION

For at least the foregoing reasons, Applicants submit that the rejections have been overcome. Therefore, claims 28-47 are in condition for allowance and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if such contact would further the examination of the present application. Please charge any shortages and credit any overcharges to our Deposit Account number 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Date: June 23, 2005



Paul A. Mendonsa
Attorney for Applicant
Reg. No. 42,879

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1026
(503) 439-8778